Access Now submission to the United Nations
on the Universal Periodic Review - 2018 Cycle

China

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action-oriented global community, as through our RightsCon Summit Series, and our technology arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to human rights that protects user rights, including privacy and freedom of expression. Access Now has worked extensively on digital rights including commenting on the ruling on free expression and web blocking, protection of Net Neutrality and government shutdowns of communications networks.

Domestic and international human rights obligations

3. China is a signatory to various international human rights instruments, which include the International Covenant on Civil and Political Rights (ICCPR), the Convention against Torture (CAT), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW).
4. Article 35 of the Chinese constitution recognizes citizens' freedom of speech, of press, and of assembly.
5. The Chinese Constitution in article 40 provides individuals with the right to privacy and protects this right from interference except in circumstances of national security, criminal investigation, and public security.

Violations of access to information & freedom of expression

7. In 2016, Freedom House ranked China as "the worst abuser of internet freedom."
8. The Chinese government undermines access to information by imposing broad bans on online content and seeking to penalize internet intermediaries.[1] In order to comply with the government's stringent content management policies, companies are required to spend 20 to 30 percent of their labor cost on auditing content.

1 https://www.cnn.com/2017/07/21/asia/china-internet-censorship/index.html

9. The Chinese Cybersecurity law is alarming given the potential of abuse by the Chinese government. Pursuant to the Cybersecurity Law, the Chinese government has the power to order the deletion or closure of websites and social media accounts.
10. On August 11, 2017 the Chinese Cyberspace Administration, which is the government's internet regulator, investigated three social media platforms, Tencent, Baidu, and Sina, for violating the Cybersecurity law. The government alleged that these companies failed to manage illegal content uploaded by their users.[2]
11. In December 2014 a leaked email from the Internet Information Office of Zhanggong District revealed the Chinese government's use of troll armies in order to shape online discourse and silence dissenting voices.
12. In 2017, the government implemented new measures to restrict the use of VPNs as a tool to circumvent online censorship.[3] VPN are an essential tool for internet users not only to access content globally, but also to protect the privacy of their connections and traffic.
13. Intentional disruptions of access to apps, services, and platforms appear to occur during sensitive political events. For instance, users of messaging app WhatsApp reported throttling and other disruptions of access to that platform in the wake of the death of Chinese Nobel Peace Prize laureate Liu Xiaobo.[4]
14. More broadly, Chinese officials have promoted visions of internet governance that fail to accord with the multi-stakeholder nature of global communications networks. Concepts like "Internet sovereignty," pushed by China at the Ten Year Review of the World Summit on the Information Society in 2015,[5] looks to assert government and multi-lateral control over the oversight, design, and growth of the global internet, to the detriment of civil society and private sector stakeholders.

Developments of digital rights in China

15. Pursuant to the 2015 Counterterrorism Law, the government can requires that all internet providers retain their ability to access communications. This law effectively bans end-to-end encryption. The law also imposes a duty on providers to monitor their site for "terrorist or extremist content", as well as block and report this type of content. A party who fails to comply with this law will be subject to a fine for a "serious" violation, which has no upper limit. Because of the hefty

[2] https://thediplomat.com/2017/08/china-accuses-its-top-3-internet-giants-of-potentially-violating-cybersecurity-law/
[3] https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february
[4] https://www.cnn.com/2017/07/21/asia/china-internet-censorship/index.html
[5] https://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html

fines, certain companies spend 20 to 30 percent of their labor cost on auditing content.

16. In November 2016, the government passed the Cybersecurity Law (CSL), which went into effect on June 1, 2017. This law applies to network operators, including network owners, administrators, and service providers that maintain computer networks. The CyberSecurity law also reinforces the government's data localization agenda by requiring network operators to store information in China.
17. Many provisions in the CSL have a direct negative impact on the exercise of human rights in China. For example, Article 50 gives the government the authority to cut off access to media platforms overseas that disseminate information that is broadly banned under Chinese laws and regulations.[6] Article 58 empowers the government to limit internet connections when authorities see the need to "safeguard national security and social public order." However, among the provisions, two in particular -- Article 24 on real-name registration and Article 37 on data localization -- stand out not only because they threaten human rights, but also because they have highly questionable value for cybersecurity. In fact, these provisions may undermine cybersecurity.
18. Article 24 of the CSL[7] mandates that network operators, specifically those classified as providers of publication/messaging systems, register users under their legal name; and if an individual fails to provide a real name, the individual cannot get access to services. This type of policy is typically used to "encourage" people to self-censor before they speak out online. Indeed, according to an official government press outlet, Xinhua News, the policy is intended to ensure a safe, good-faith environment online since publishing under their own names would make Chinese netizens more cautious about what they say.[8]
19. Within Article 37 is the requirement that critical information infrastructure operators store personal information and important data domestically, with "security assessments" necessary to transfer any such data abroad. This practice is known as data localization. Governments promote this type of requirement as a way to keep data out of the reach of foreign governments and ensure that the information is better protected.[9] While data localization might seem like a way to provide security, in practice it has typically been used to increase government monitoring of people's online activities.[10] The impact of a policy like this is even worse in countries with a record of systematic human rights violations.
20. On February 28, 2018, CNN reported that Apple moved iCloud accounts to mainland China to Guizhou-Cloud Big Data (GCBD), a state-run Chinese

[6] https://en.wikipedia.org/wiki/Censorship_in_China
[7] http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en
[8] http://news.xinhuanet.com/politics/2017-05/31/c_1121064385.htm
[9] http://www.slate.com/articles/technology/future_tense/2017/11/countries_are_increasingly_imposing_borders_on_the_cloud.html
[10] https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/

servers. [11] Registered Chinese iCloud users' information will be sent to GCBD[12] among with the digital keys needed to unblock the information.[13]

21. Previously, in order for the Chinese authorities to access Apple users' accounts, they had to go through an international legal process and adhere to U.S. laws on users rights.[14] Now, because the Chinese government has both the iCloud data and the cryptographic keys they no longer have to go through this process.[15] Chinese scholars have highlighted that Chinese law does not afford the same protections as U.S. law. Specifically, Chinese law does not require court approval; and the police can issue and execute a warrant.

Recommendations

22. China can improve its human rights record and treatment of digital rights in several areas. We recommend that the government of China:
    a. Commit to enhancing freedom of expression online and preventing violations by state and non-state actors;
    b. Commit to refrain from blocking and censorshing online communication unless strictly necessary for national security purposes, and proportionate to achieving a legitimate aim under the ICCPR;
    c. Refrain from enacting legislation that imposes sanctions on internet intermediaries for third-party content;
    d. Review existing legislation, including the Cybersecurity Law, and amend in line with international human rights law and norms, including by eliminating data localization and real name requirements;
    e. Enact laws and telecommunications regulations protecting access to information and freedom of expression rights;
    f. Strengthen cooperation with United Nations treaty mechanisms and issue standing invitations to UN special procedures such as the UN special rapporteurs on freedom of expression and the right to privacy; and
    g. Permit the use of end-to-end encrypted applications and Virtual Private Networks (VPN) without licensing or registration requirements.

[11] http://money.cnn.com/2018/02/28/technology/apple-icloud-data-china/index.html
[12] https://www.nytimes.com/2018/01/23/opinion/apple-china-data.html
[13] https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060
[14] http://money.cnn.com/2018/02/28/technology/apple-icloud-data-china/index.html
[15] http://money.cnn.com/2018/02/28/technology/apple-icloud-data-china/index.html